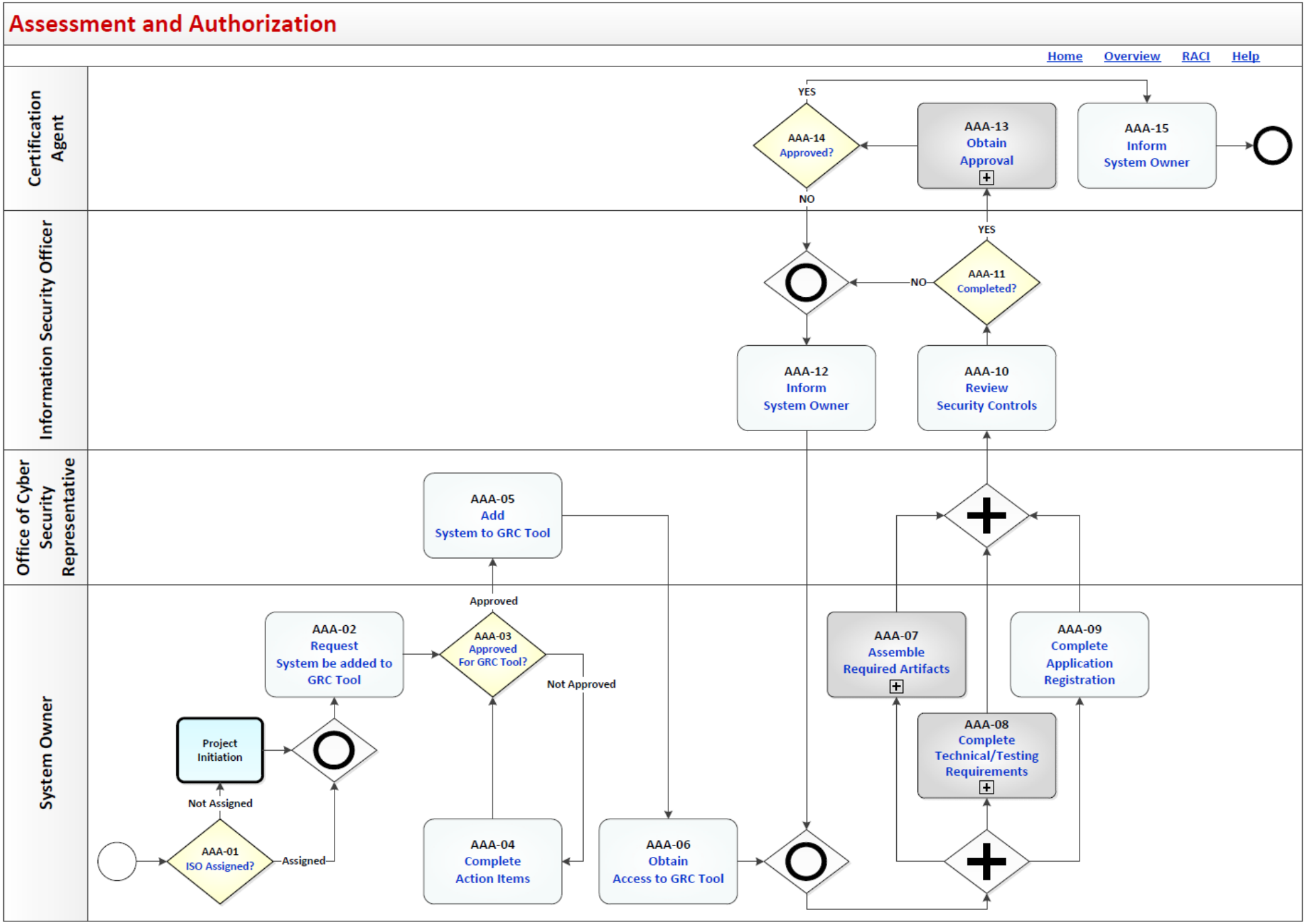
Assessment and Authorization

ProPath

Office of Information and Technology

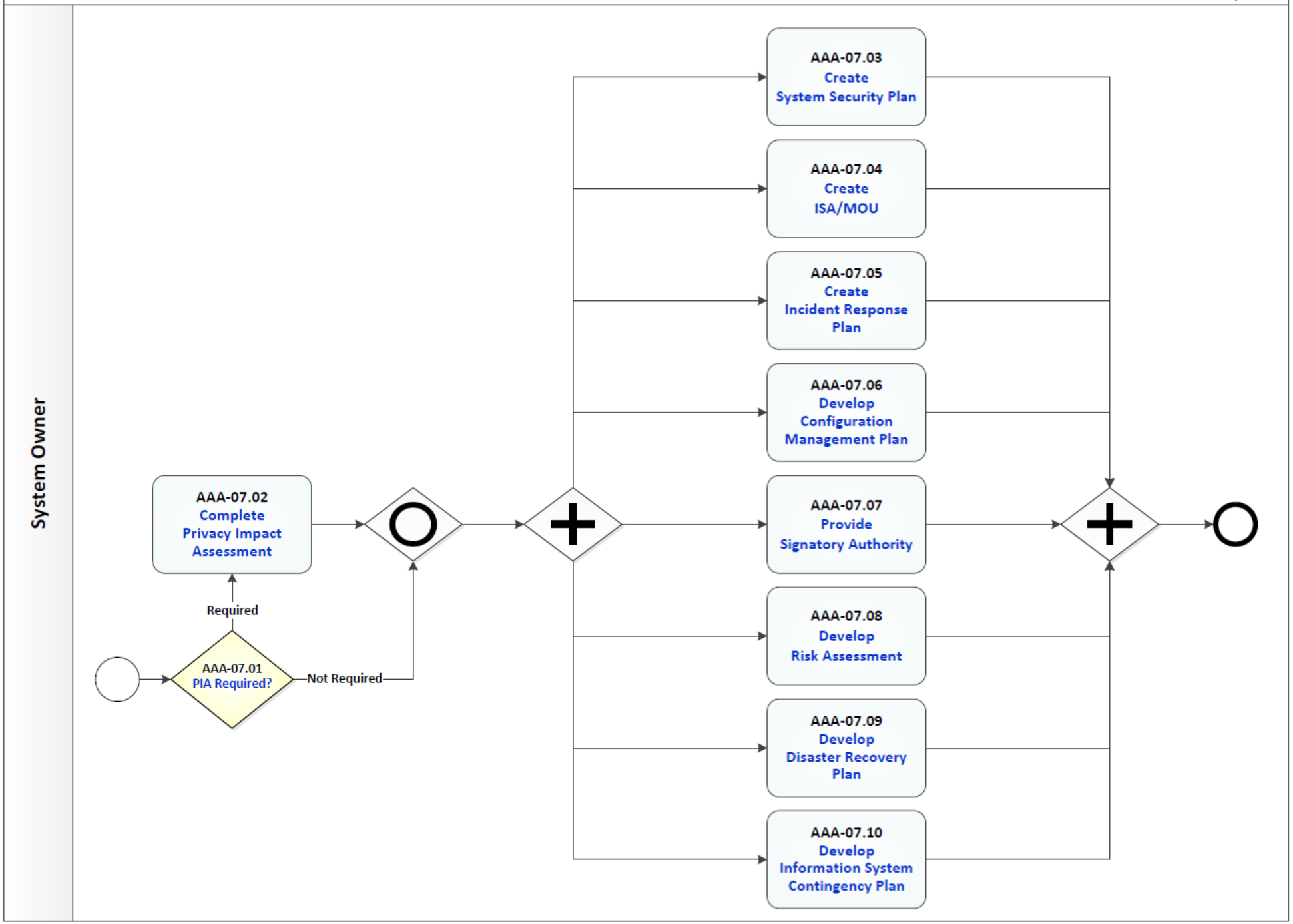
Table of Contents

Assessment and Authorization Process Maps



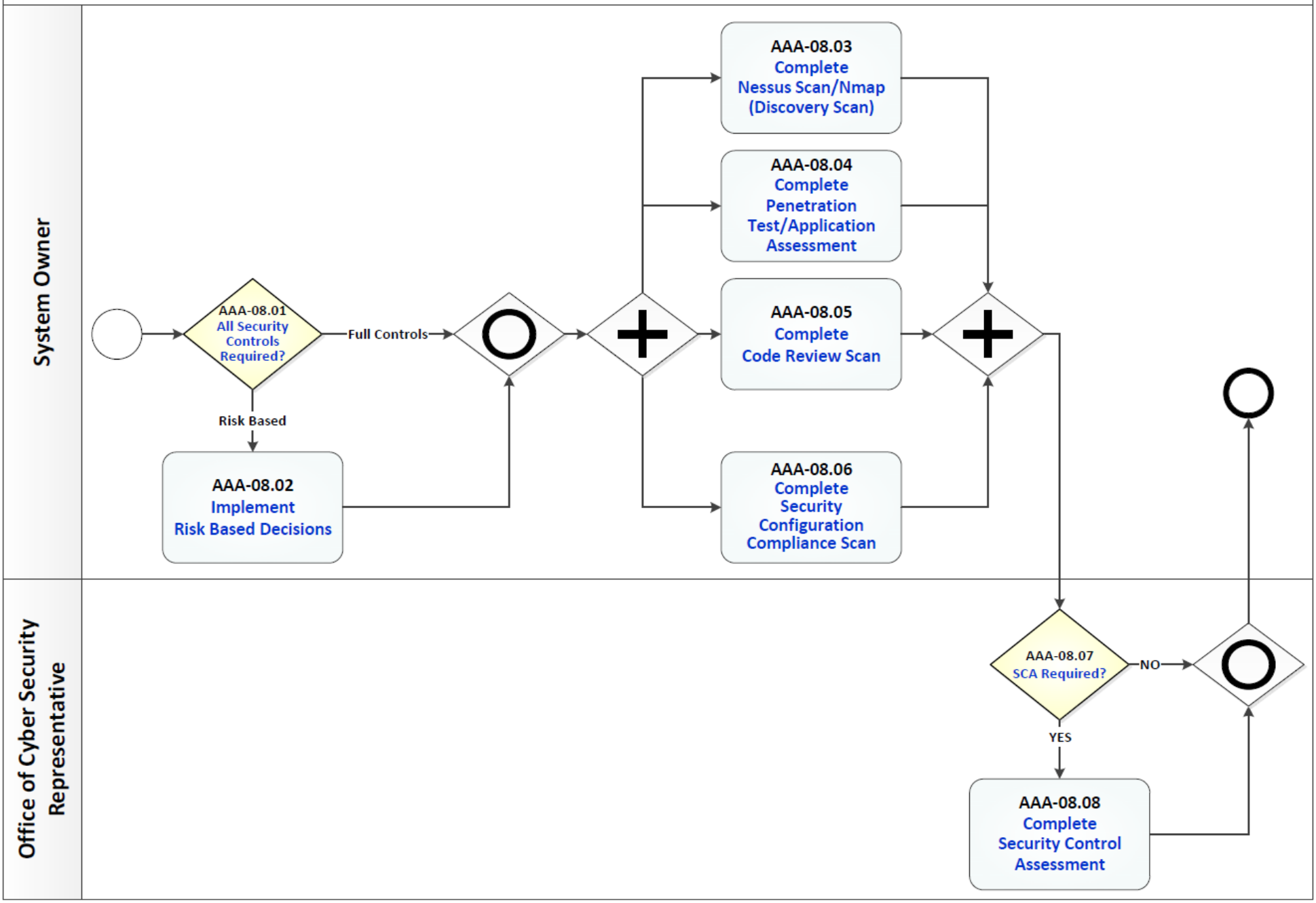
The links in this process map are inactive. Please scroll to view activity data.

Assessment and Authorization: AAA-07 Assemble Required Artifacts

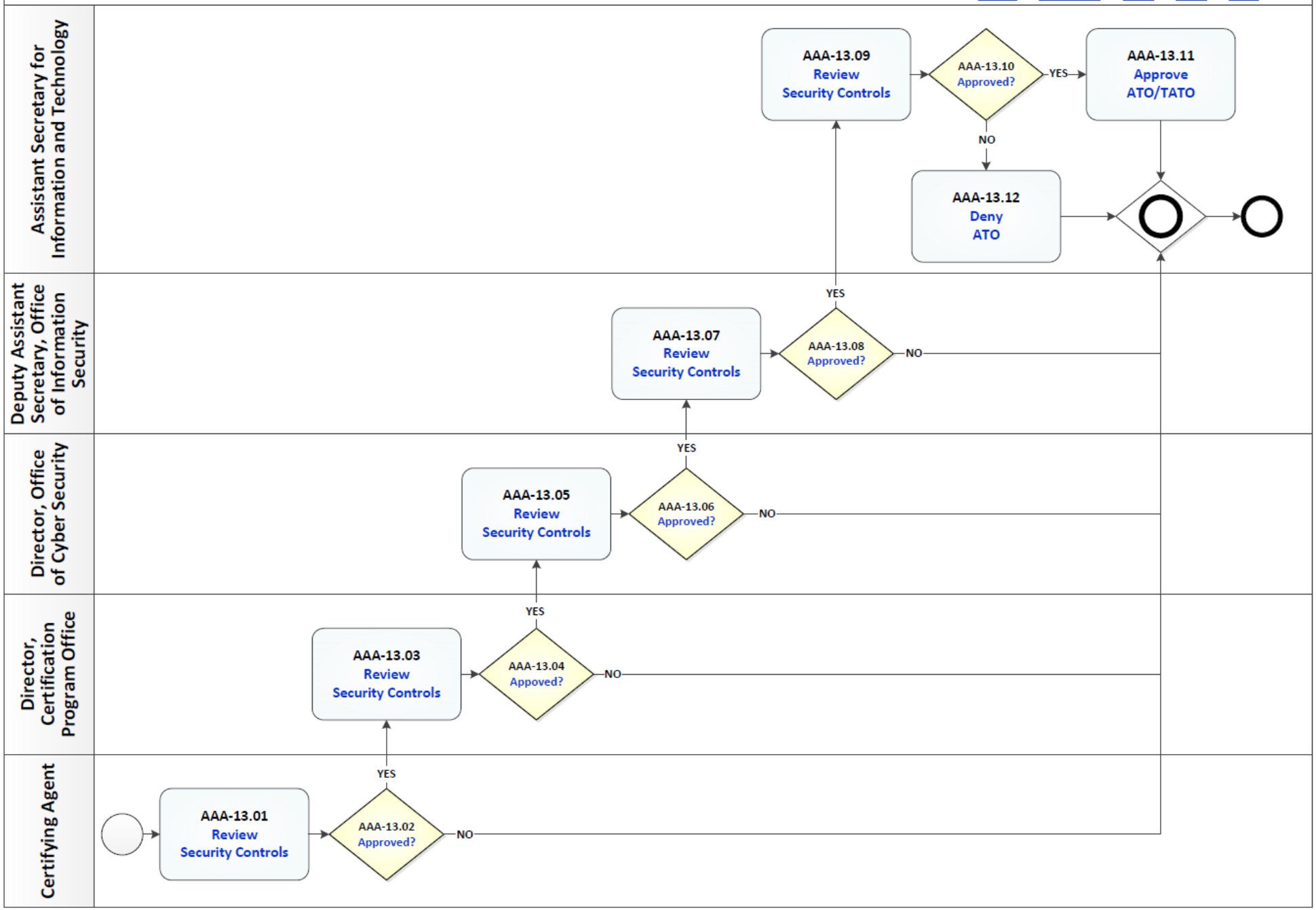


The links in this process map are inactive. Please scroll to view activity data.

Assessment and Authorization: AAA-08 Complete Technical/Testing Requirements



Assessment and Authorization: AAA-13 Obtain Approval



Process: Assessment and Authorization

Overview: The process map for Assessment and Authorization cycles through the following process and review activities:

AAA-01 ISO Assigned?
AAA-02 Request System to be Added to the GRC Tool
AAA-03 Approved for GRC Tool?
AAA-04 Complete Action Items
AAA-05 Add System to the GRC Tool
AAA-06 Obtain Access to the GRC Tool
AAA-07 Assemble Required Artifacts
AAA-07.01 PIA Needed?
AAA-07.02 Complete Privacy Impact Assessment
AAA-07.03 Create System Security Plan
AAA-07.04 Create ISA/MOU
AAA-07.05 Create Incident Response Plan
AAA-07.06 Develop Configuration Management Plan
AAA-07.07 Provide Signatory Authority
AAA-07.08 Develop Risk Assessment
AAA-07.09 Develop Disaster Recovery Plan
AAA-07.10 Develop Information System Contingency Plan
AAA-08 Complete Technical/Testing Requirements
AAA-08.01 All Security Controls Required?
AAA-08.02 Implement Risk Based Decisions Process
AAA-08.03 Complete Nessus Scan/Nmap (Discovery Scan)
AAA-08.04 Complete Code Review Scan
AAA-08.05 Complete Penetration Test/Application Assessment
AAA-08.06 Complete Security Configuration Compliance Scan
AAA-08.07 SCA Required?
AAA-08.08 Complete Security Control Assessment
AAA-09 Complete Application Registration
AAA-10 Review Security Controls
AAA-11 Completed?
AAA-12 Inform System Owner
AAA-13 Obtain Approval
AAA-13.01 Review Security Controls
AAA-13.02 Approved?
AAA-13.03 Review Security Controls
AAA-13.04 Approved?
AAA-13.05 Review Security Controls
AAA-13.06 Approved?
AAA-13.07 Review Security Controls
AAA-13.08 Approved?
AAA-13.09 Review Security Controls
AAA-13.10 Approved?
AAA-13.11 Deny ATO

AAA-13.12 Approve ATO/TATO
AAA-14 Approved?
AAA-15 Inform System Owner of ATO Status

Assessment and Authorization Description and Goals

Description

The Assessment and Authorization process describes the end to end process for ensuring new VA information systems adhere to and are in compliance with Federal Information Security Management Act (FISMA). The purpose of an Authority To Operate (ATO) is to ensure the risks to VA (operations, assets, or individuals) are acceptable. The result is the issuance of an ATO. If the risk to Agency operations, assets or individuals is low, an ATO authorizes the system to be moved into production or use production data.

Throughout the Assessment and Authorization process System Owner work with their assigned Information Security Officer (ISO) to obtain an ATO. The process entails gaining access to the Governance, Risk and Compliance (GRC) tool, RiskVision, to serve as the management tool for the A&A process. The GRC tool is used to document accreditation requirements including technical testing/scans, security documentation, and actions identified during the Security Control Assessment. The completion of the required security documentation and technical tests enable the Office of Cyber Security (OCS) Certification Program Office (CPO) to determine the final risk to VA based on the vulnerabilities in the information system; assess any planned, completed, or corrective actions to reduce or eliminate those vulnerabilities; make a final determination on the acceptability of risk to VA; and prepare the final accreditation decision letter.

The complete set of accreditation requirements including technical test and security documentations are enumerated in the “Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures”.

Once the accreditation requirements are met and submitted in RiskVision, the results are reviewed and approved by the Certification Agent, Directors of CPO and OCS, Deputy Assistant Secretary Office of Information Security, and finally Assistant Secretary for Information and Technology who grants or denies the Authority to Operate.

Goals

The Goal of the Assessment and Authorization process is to ensure compliance with Agency information security policy and in support of the Federal Information Security Management Act (FISMA), and the attainment of an ATO for new systems.

Assessment and Authorization RACI Information

The following describes the RACI information for this process:

AAA-01 ISO Assigned?

Responsible Role: System Owner
Accountable Role: Office of Cyber Security Representative
Consulted Role: None Listed
Informed: None Listed

AAA-02 Request System to be Added to the GRC Tool

Responsible Role: System Owner
Accountable Role: Office of Cyber Security Representative
Consulted Role: None Listed
Informed: None Listed

AAA-03 Approved for GRC Tool?

Responsible Role: System Owner
Accountable Role: Office of Cyber Security Representative
Consulted Role: None Listed
Informed: None Listed

AAA-04 Complete Action Items

Responsible Role: System Owner
Accountable Role: Office of Cyber Security Representative
Consulted Role: None Listed
Informed: None Listed

AAA-05 Add System to the GRC Tool

Responsible Role: Office of Cyber Security Representative

Accountable Role: Office of Cyber Security Representative
Consulted Role: None Listed
Informed: None Listed

AAA-06 Obtain Access to the GRC Tool

Responsible Role: System Owner
Accountable Role: Office of Cyber Security Representative
Consulted Role: None Listed
Informed: None Listed

AAA-07.01 PIA Needed?

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-07.02 Complete Privacy Impact Assessment

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: Privacy Officer
Informed: None Listed

AAA-07.03 Create System Security Plan

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-07.04 Create ISA/MOU

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-07.05 Create Incident Response Plan

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-07.06 Develop Configuration Management Plan

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-07.07 Provide Signatory Authority

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-07.08 Develop Risk Assessment

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-07.09 Develop Disaster Recovery Plan

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-07.10 Develop Information System Contingency Plan

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-08.01 All Security Controls Required?

Responsible Role: System Owner
Accountable Role: Office of Cyber Security Representative
Consulted Role: None Listed
Informed: None Listed

AAA-08.02 Implement Risk Based Decisions Process

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-08.03 Complete Nessus Scan/Nmap (Discovery Scan)

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-08.04 Complete Code Review Scan

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-08.05 Complete Penetration Test/Application Assessment

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-08.06 Complete Security Configuration Compliance Scan

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-08.07 SCA Required?

Responsible Role: Office of Cyber Security Representative
Accountable Role: Information Security Officer
Consulted Role: None Listed
Informed: None Listed

AAA-08.08 Complete Security Control Assessment

Responsible Role: Office of Cyber Security Representative
Accountable Role: Information Security Officer
Consulted Role: None Listed

Informed: None Listed

AAA-09 Complete Application Registration

Responsible Role: System Owner
Accountable Role: Information Security Officer
Consulted Role: Office of Cyber Security Representative
Informed: Director, Certification Program Office; Director, Office of Cyber Security

AAA-10 Review Security Controls

Responsible Role: Information Security Officer
Accountable Role: Certification Agent
Consulted Role: None Listed
Informed: None Listed

AAA-11 Completed?

Responsible Role: Information Security Officer
Accountable Role: Certification Agent
Consulted Role: None Listed
Informed: None Listed

AAA-12 Inform System Owner

Responsible Role: Information Security Officer
Accountable Role: Certification Agent
Consulted Role: None Listed
Informed: None Listed

AAA-13.01 Review Security Controls

Responsible Role: Certification Agent
Accountable Role: Director, Certification Program Office

Consulted Role: None Listed
Informed: None Listed

AAA-13.02 Approved?

Responsible Role: Certification Agent
Accountable Role: Director, Certification Program Office
Consulted Role: None Listed
Informed: None Listed

AAA-13.03 Review Security Controls

Responsible Role: Director, Certification Program Office
Accountable Role: Director, Office of Cyber Security
Consulted Role: None Listed
Informed: None Listed

AAA-13.04 Approved?

Responsible Role: Director, Certification Program Office
Accountable Role: Director, Office of Cyber Security
Consulted Role: None Listed
Informed: None Listed

AAA-13.05 Review Security Controls

Responsible Role: Director, Office of Cyber Security
Accountable Role: Deputy Assistant Secretary, Office of Information Security
Consulted Role: None Listed
Informed: None Listed

AAA-13.06 Approved?

Responsible Role: Director, Office of Cyber Security

Accountable Role: Deputy Assistant Secretary, Office of Information Security
Consulted Role: None Listed
Informed: None Listed

AAA-13.07 Review Security Controls

Responsible Role: Deputy Assistant Secretary, Office of Information Security
Accountable Role: Assistant Secretary for Information and Technology
Consulted Role: None Listed
Informed: None Listed

AAA-13.08 Approved?

Responsible Role: Deputy Assistant Secretary, Office of Information Security
Accountable Role: Assistant Secretary for Information and Technology
Consulted Role: None Listed
Informed: None Listed

AAA-13.09 Review Security Controls

Responsible Role: Assistant Secretary for Information and Technology
Accountable Role: Assistant Secretary for Information and Technology
Consulted Role: None Listed
Informed: None Listed

AAA-13.10 Approved?

Responsible Role: Assistant Secretary for Information and Technology
Accountable Role: Assistant Secretary for Information and Technology
Consulted Role: None Listed
Informed: None Listed

AAA-13.11 Deny ATO

Responsible Role: Assistant Secretary for Information and Technology
Accountable Role: Assistant Secretary for Information and Technology
Consulted Role: None Listed
Informed: None Listed

AAA-13.12 Approve ATO/TATO

Responsible Role: Assistant Secretary for Information and Technology
Accountable Role: Assistant Secretary for Information and Technology
Consulted Role: None Listed
Informed: None Listed

AAA-14 Approved?

Responsible Role: Certification Agent
Accountable Role: Director, Certification Program Office
Consulted Role: None Listed
Informed: None Listed

AAA-15 Inform System Owner of ATO Status

Responsible Role: Certification Agent
Accountable Role: Director, Certification Program Office
Consulted Role: None Listed
Informed: None Listed

Assessment and Authorization Associated Artifacts Information

Associated Artifacts information (including hyperlinks) for this process includes:

Authority to Operate

Code Review Questionnaire Template

Disaster Recovery Plan Template

Incident Response Plan Template

Information System Contingency Plan Template

Interconnection Security Agreement/Memorandum of Understanding Template

Local Risk Based Decision Memorandum

OIS Risk Based Decision Memorandum

OIS V and V Secure Code Review Validation Request Form Template

Penetration Test Questionnaire Template

Privacy Impact Assessment Template

Risk Assessment

RiskVision System Information Form Template

RiskVision System Inventory Checklist

Signatory Authority Template

Supplemental Vulnerability Scan Request Template

System Configuration Management Plan Template

System Security Plan

Assessment and Authorization Tools and Web Sites Information

The Tools and Web Sites associated with this process (including hyperlinks) include:

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Business Continuity Portal

HP Fortify Static Code Analyzer (SCA)

ISA/MOU Document Review Site

Office of Cyber Security (OCS) Portal

Office of Information Security Portal

Office of Information Security Risk Based Decisions Portal

OIS Software Assurance Portal

PD Information Assurance

Privacy Impact Assessments Portal

Risk Management and Incident Response (RMIR) Portal

Technical Services Project Repository (TSPR)

Assessment and Authorization Standards Information

Standards associated with this process (including hyperlinks) include:

Bulletin FSS No. 96, Types of Risk Based Decisions

Field Security Service No 124 Bulletin MOU/ISA Document Processing: FINAL Guidance

Information Access and Privacy Program

NIST Special Publication 800-18 - Guide for Developing Security Plans for Federal Information Systems

NIST Special Publication 800-30 - Guide for Conducting Risk Assessments

NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems

NIST Special Publication 800-47 - Security Guide for Interconnecting Information Technology Systems

NIST Special Publication 800-61 - Computer Security Incident Handling Guide

NIST Special Publication 800-70 - National Checklist Program for IT Products—Guidelines for Checklist Users

Office of Information Security Risk Based Decision Standard Operating Procedures

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

Secure Code Review Standard Operating Procedure

Software Assurance Program Memorandum (VAIQ 7477488)

Software Configuration Management Plan Standard

VA Common Application Enumeration

VA Directive 6502, VA Enterprise Privacy Program

VA Directive 6508, Privacy Impact Assessments

VA Handbook 6500, Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program

VA Handbook 6500.3, Certification and Accreditation of Federal Information Systems

VA Handbook 6500.8, Information System Contingency Planning

VA Handbook 6508.1, Privacy Impact Assessment

Assessment and Authorization Process

Process Activity Name: AAA-01 ISO Assigned?

Previous Activities

Process Begins

Next Activities

If "Assigned":

AAA-02 Request System to be Added to the GRC Tool

Or

If "Not Assigned":

Project Initiation Process

Description

The System Owner determines if an ISO is assigned.

Responsible Role

System Owner

Accountable Role

Office of Cyber Security Representative

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-02 Request System to be Added to the GRC Tool

Previous Activities

AAA-01 ISO Assigned?

Or

Project Initiation Process

Next Activities

AAA-03 Approved for GRC Tool?

Description

The System Owner contacts the Governance, Risk and Compliance (GRC) RiskVision Working Group to request the system to be added to the agenda for a RiskVision Working Group Meeting. The RiskVision Working Group provides the System Owner with the necessary forms that must be completed and submitted prior to the RiskVision Working Group meeting. The RiskVision

Working Group Meeting decides whether to move forward with the addition of the system into RiskVision or recommends continuing the discussion with assigned action items.

Input

System Information

Stakeholder Login Information

Output

RiskVision System Inventory Checklist

RiskVision System Information Form

Pending Action Items

Associated Artifacts

RiskVision System Inventory Checklist

RiskVision System Information Form Template

Responsible Role

System Owner

Accountable Role

Office of Cyber Security Representative

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Office of Cyber Security (OCS) Portal

Office of Information Security Portal

Standards

None Listed

More Info

The RiskVision Working Group can be contact via mail group VA RISK VISION WG.

Process Activity Name: AAA-03 Approved for GRC Tool?

Previous Activities

AAA-02 Request System to be Added to the GRC Tool

Next Activities

If "Not Approved":

AAA-04 Complete Action Items

Or

If "Approved":

AAA-05 Add System to the GRC Tool

Description

It is determined if the system is approved to be added to the GRC tool. If not approved, the review board will assign the system owner further action items.

Responsible Role

System Owner

Accountable Role

Office of Cyber Security Representative

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-04 Complete Action Items

Previous Activities

AAA-03 Approved for GRC Tool?

Next Activities

AAA-03 Approved for GRC Tool?

Description

The System Owner resolves and completes the action items submitted by the RiskVision Working Group in order to obtain approval for the addition of the system to RiskVision, and submits the completed action items to the RiskVision Working Group for reconsideration.

Input

Pending Action Items

Output

Completed Action Items

Request to be added to RiskVision Working Group Agenda

Associated Artifacts

None Listed

Responsible Role

System Owner

Accountable Role

Office of Cyber Security Representative

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

None Listed

Standards

None Listed

More Info

None Listed

Process Activity Name: AAA-05 Add System to the GRC Tool

Previous Activities

AAA-03 Approved for GRC Tool?

Next Activities

AAA-06 Obtain Access to the GRC Tool

Description

Office of Cyber Security (OCS) Representative notifies the System Owner that the request to add the system to the Governance, Risk and Compliance (GRC) tool, RiskVision, has been approved by the RiskVision Working Group and the system has been added to RiskVision.

Input

RiskVision System Inventory Checklist

RiskVision System Information Form

Output

System Added to GRC Tool

Associated Artifacts

None Listed

Responsible Role

Office of Cyber Security Representative

Accountable Role

Office of Cyber Security Representative

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

None Listed

More Info

The RiskVision Enterprise Operations Instance is managed by the Austin Center.

Process Activity Name: AAA-06 Obtain Access to the GRC Tool

Previous Activities

AAA-05 Add System to the GRC Tool

Next Activities

AAA-07 Assemble Required Artifacts

And

AAA-08 Complete Technical/Testing Requirements

And

AAA-09 Complete Application Registration

Description

The System Owner contacts the Governance, Risk and Compliance (GRC) Service Desk at mail group VA GRC Service Desk to obtain access and user accounts to RiskVision tool for the designated stakeholders.

Input

Request for RiskVision Access

Output

RiskVision Access for Stakeholders

Associated Artifacts

None Listed

Responsible Role

System Owner

Accountable Role

Office of Cyber Security Representative

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

None Listed

More Info

None Listed

Process Activity Name: AAA-07 Assemble Required Artifacts

Concurrent Activities

AAA-08 Complete Technical/Testing Requirements

And

AAA-09 Complete Application Registration

Previous Activities

AAA-06 Obtain Access to the GRC Tool

Or

AAA-12 Inform System Owner

Next Activities

AAA-07.01 PIA Needed?

Description

This group of activities assembles all the required artifacts for submission for the ATO package

Process Activity Name: AAA-07.01 PIA Needed?

Previous Activities

AAA-07 Assemble Required Artifacts

Next Activities

If "Required":

AAA-07.02 Complete Privacy Impact Assessment

Or

If "Not Required":

AAA-07.03 Create System Security Plan

And

AAA-07.04 Create ISA/MOU

And

AAA-07.05 Create Incident Response Plan

And

AAA-07.06 Develop Configuration Management Plan

And

AAA-07.07 Provide Signatory Authority

And

AAA-07.08 Develop Risk Assessment

And

AAA-07.09 Develop Disaster Recovery Plan

And

AAA-07.10 Develop Information System Contingency Plan

Description

It is determined whether a Privacy Impact Assessment is required.

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-07.02 Complete Privacy Impact Assessment

Previous Activities

AAA-07.01 PIA Needed?

Next Activities

AAA-07.03 Create System Security Plan

And

AAA-07.04 Create ISA/MOU

And

AAA-07.05 Create Incident Response Plan

And

AAA-07.06 Develop Configuration Management Plan

And

AAA-07.07 Provide Signatory Authority

And

AAA-07.08 Develop Risk Assessment

And

AAA-07.09 Develop Disaster Recovery Plan

And

AAA-07.10 Develop Information System Contingency Plan

Description

The System Owner works with Privacy Officer and Information Security Officer (ISO) to develop the Privacy Impact Assessment (PIA) based on the outcome of a developed Privacy Threshold Analysis. The PIA, if needed, must be completed and submitted to the Privacy Services Office and any further comments by the Privacy Services analysts are incorporated into the PIA. Once the Privacy Officer verifies PIA as complete, the System Owner submits PIA as an Adobe PDF file with the signatures of the System Owner, Privacy Officer, ISO, and any other relevant stakeholders to PIASupport@va.gov. The System Owner or delegate then uploads the PIA in the GRC tool, RiskVision.

Input

Privacy Threshold Analysis

Output

Privacy Impact Assessment

Associated Artifacts

Privacy Impact Assessment Template

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

Privacy Officer

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Privacy Impact Assessments Portal

Office of Cyber Security (OCS) Portal

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

VA Directive 6502, VA Enterprise Privacy Program

VA Directive 6508, Privacy Impact Assessments

VA Handbook 6508.1, Privacy Impact Assessment

More Info

None Listed

Process Activity Name: AAA-07.03 Create System Security Plan

Concurrent Activities

AAA-07.04 Create ISA/MOU

And

AAA-07.05 Create Incident Response Plan

And

AAA-07.06 Develop Configuration Management Plan

And

AAA-07.07 Provide Signatory Authority

And

AAA-07.08 Develop Risk Assessment

And

AAA-07.09 Develop Disaster Recovery Plan

And

AAA-07.10 Develop Information System Contingency Plan

Previous Activities

AAA-07.01 PIA Needed?

Or

AAA-07.02 Complete Privacy Impact Assessment

Next Activities

AAA-10 Review Security Controls

Description

The System Owner or delegate/System Steward works with the assigned Information Security Officer (ISO) to create the System Security Plan (SSP) in the Governance, Risk and Compliance (GRC) tool, RiskVision. The SSP ensures that the planned or existing security controls are fully documented. The SSP provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Input

System Classification/Category

System Information

System Security Controls

Output

System Security Plan

Associated Artifacts

None Listed

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

NIST Special Publication 800-18 - Guide for Developing Security Plans for Federal Information Systems

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

VA Handbook 6500.3, Certification and Accreditation of Federal Information Systems

More Info

None Listed

Process Activity Name: AAA-07.04 Create ISA/MOU

Concurrent Activities

AAA-07.03 Create System Security Plan

And

AAA-07.05 Create Incident Response Plan

And

AAA-07.06 Develop Configuration Management Plan

And

AAA-07.07 Provide Signatory Authority

And

AAA-07.08 Develop Risk Assessment

And

AAA-07.09 Develop Disaster Recovery Plan

And

AAA-07.10 Develop Information System Contingency Plan

Previous Activities

AAA-07.01 PIA Needed?

Or

AAA-07.02 Complete Privacy Impact Assessment

Next Activities

AAA-10 Review Security Controls

Description

The System Owner works with Information Security Officer (ISO) to create the Interconnection Security Agreement/Memorandum of Understanding (ISA/MOU). An ISA/MOU is provided for all external interconnections. Once Completed, System Owner, a delegate, or the ISO uploads

all ISA/MOUs to ISA/MOU Document Review Site. Once completed, the System Owner, or designee, uploads the signed ISA/MOU into RiskVision.

Input

System Security Plan

Output

Interconnection Security Agreement/Memorandum of Understanding

Associated Artifacts

Interconnection Security Agreement/Memorandum of Understanding Template

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

ISA/MOU Document Review Site

Office of Cyber Security (OCS) Portal

Standards

Field Security Service No 124 Bulletin MOU/ISA Document Processing: FINAL Guidance

NIST Special Publication 800-47 - Security Guide for Interconnecting Information Technology Systems

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

VA Handbook 6500.3, Certification and Accreditation of Federal Information Systems

More Info

None Listed

Process Activity Name: AAA-07.05 Create Incident Response Plan

Concurrent Activities

AAA-07.03 Create System Security Plan

And

AAA-07.04 Create ISA/MOU

And

AAA-07.06 Develop Configuration Management Plan

And

AAA-07.07 Provide Signatory Authority

And

AAA-07.08 Develop Risk Assessment

And

AAA-07.09 Develop Disaster Recovery Plan

And

AAA-07.10 Develop Information System Contingency Plan

Previous Activities

AAA-07.01 PIA Needed?

Or

AAA-07.02 Complete Privacy Impact Assessment

Next Activities

AAA-10 Review Security Controls

Description

The System Owner works with the assigned Information Security Officer (ISO) to create the Incident Response Plan (IRP). An Incident Response Plan is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Once completed and tested, the System Owner, or designee, uploads the signed Incident Response Plan into RiskVision.

Input

Risk Assessment

System Security Plan

Output

Incident Response Plan

Associated Artifacts

Incident Response Plan Template

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Business Continuity Portal

Office of Cyber Security (OCS) Portal

Standards

Information Access and Privacy Program

NIST Special Publication 800-61 - Computer Security Incident Handling Guide

VA Handbook 6500.3, Certification and Accreditation of Federal Information Systems

More Info

None Listed

Process Activity Name: AAA-07.06 Develop Configuration Management Plan

Concurrent Activities

AAA-07.03 Create System Security Plan

And

AAA-07.04 Create ISA/MOU

And

AAA-07.05 Create Incident Response Plan

And

AAA-07.07 Provide Signatory Authority

And

AAA-07.08 Develop Risk Assessment

And

AAA-07.09 Develop Disaster Recovery Plan

And

AAA-07.10 Develop Information System Contingency Plan

Previous Activities

AAA-07.01 PIA Needed?

Or

AAA-07.02 Complete Privacy Impact Assessment

Next Activities

AAA-10 Review Security Controls

Description

The System Owner develops the Configuration Management Plan (CMP) which identifies configuration management roles and responsibilities, resources, and processes to ensure any changes to a General Support System or a Major Application are evaluated and approved before implementation. This Plan includes roles, responsibilities, resources, communication methods, system configuration baseline, and configuration control and change management processes. The CMP should include baseline configurations for each Operating System, database, application, and network devices. Once completed, the System Owner uploads the CMP to RiskVision.

Input

System Security Plan

Output

System Configuration Management Plan

Associated Artifacts

System Configuration Management Plan Template

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

NIST Special Publication 800-70 - National Checklist Program for IT Products—Guidelines for Checklist Users

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

Software Configuration Management Plan Standard

VA Handbook 6500.3, Certification and Accreditation of Federal Information Systems

More Info

None Listed

Process Activity Name: AAA-07.07 Provide Signatory Authority

Concurrent Activities

AAA-07.03 Create System Security Plan

And

AAA-07.04 Create ISA/MOU

And

AAA-07.05 Create Incident Response Plan

And

AAA-07.06 Develop Configuration Management Plan

And

AAA-07.08 Develop Risk Assessment

And

AAA-07.09 Develop Disaster Recovery Plan

And

AAA-07.10 Develop Information System Contingency Plan

Previous Activities

AAA-07.01 PIA Needed?

Or

AAA-07.02 Complete Privacy Impact Assessment

Next Activities

AAA-10 Review Security Controls

Description

The System Owner completes the Signatory Authority form signed and dated by appropriate parties. System Owner or delegate uploads the completed Signatory Authority into RiskVision.

Once completed, the System Owner, or designee, uploads the signed Signatory Authority into RiskVision.

Input

Approval from RiskVision Workgroup

Output

Signatory Authority

Associated Artifacts

Signatory Authority Template

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

NIST Special Publication 800-18 - Guide for Developing Security Plans for Federal Information Systems

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

None Listed

Process Activity Name: AAA-07.08 Develop Risk Assessment

Concurrent Activities

AAA-07.03 Create System Security Plan

And

AAA-07.04 Create ISA/MOU

And

AAA-07.05 Create Incident Response Plan

And

AAA-07.06 Develop Configuration Management Plan

And

AAA-07.07 Provide Signatory Authority

And

AAA-07.09 Develop Disaster Recovery Plan

And

AAA-07.10 Develop Information System Contingency Plan

Previous Activities

AAA-07.01 PIA Needed?

Or

AAA-07.02 Complete Privacy Impact Assessment

Next Activities

AAA-10 Review Security Controls

Description

The System Owner, or designee, works with the assigned Information Security Officer (ISO) to create the Risk Assessment (RA) in the Governance, Risk and Compliance (GRC) tool, RiskVision.

Input

System Security Plan

Output

Risk Assessment

Associated Artifacts

Risk Assessment

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision National Release GRC Instance

Agiliance RiskVision Enterprise Operations GRC Instance

Office of Cyber Security (OCS) Portal

Risk Management and Incident Response (RMIR) Portal

Standards

NIST Special Publication 800-18 - Guide for Developing Security Plans for Federal Information Systems

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems

NIST Special Publication 800-30 - Guide for Conducting Risk Assessments

More Info

None Listed

Process Activity Name: AAA-07.09 Develop Disaster Recovery Plan

Concurrent Activities

AAA-07.03 Create System Security Plan

And

AAA-07.04 Create ISA/MOU

And

AAA-07.05 Create Incident Response Plan

And

AAA-07.06 Develop Configuration Management Plan

And

AAA-07.07 Provide Signatory Authority

And

AAA-07.08 Develop Risk Assessment

And

AAA-07.10 Develop Information System Contingency Plan

Previous Activities

AAA-07.01 PIA Needed?

Or

AAA-07.02 Complete Privacy Impact Assessment

Next Activities

AAA-10 Review Security Controls

Description

The System Owner or designee develops the Disaster Recovery Plan (DRP) as the entry point for the creation of both the facility and data center plans. Once completed (and tested), the System Owner, or designee, uploads the Disaster Recovery Plan into RiskVision.

Input

Primary Site System Security Plan

Backup Site System Security Plan

Output

Disaster Recovery Plan (DRP)

Associated Artifacts

Disaster Recovery Plan Template

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Business Continuity Portal

Office of Cyber Security (OCS) Portal

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

None Listed

Process Activity Name: AAA-07.10 Develop Information System Contingency Plan

Concurrent Activities

AAA-07.03 Create System Security Plan

And

AAA-07.04 Create ISA/MOU

And

AAA-07.05 Create Incident Response Plan

And

AAA-07.06 Develop Configuration Management Plan

And

AAA-07.07 Provide Signatory Authority

And

AAA-07.08 Develop Risk Assessment

And

AAA-07.09 Develop Disaster Recovery Plan

Previous Activities

AAA-07.01 PIA Needed?

Or

AAA-07.02 Complete Privacy Impact Assessment

Next Activities

AAA-10 Review Security Controls

Description

The System Owner, or delegate, develops or revises the Information System Contingency Plan. Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods. The System Owner, or designee, uploads the Information System Contingency Plan into RiskVision.

Input

Preliminary Information System Contingency Plan

Primary Site System Security Plan

Backup Site System Security Plan

Output

Information System Contingency Plan

Associated Artifacts

Information System Contingency Plan Template

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Business Continuity Portal

Office of Cyber Security (OCS) Portal

Technical Services Project Repository (TSPR)

Standards

NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

VA Handbook 6500.8, Information System Contingency Planning

More Info

For additional guidance for completion of the ISCP refer to the Business Continuity Portal.

Process Activity Name: AAA-08 Complete Technical/Testing Requirements

Concurrent Activities

AAA-07 Assemble Required Artifacts

And

AAA-09 Complete Application Registration

Previous Activities

AAA-06 Obtain Access to the GRC Tool

Or

AAA-12 Inform System Owner

Next Activities

AAA-08.01 All Security Controls Required?

Description

This group of activities completes the technical and testing requirements to ensure the integrity of the system being analyzed.

Process Activity Name: AAA-08.01 All Security Controls Required?

Previous Activities

AAA-08 Complete Technical/Testing Requirements

Next Activities

If "Risk Based":

AAA-08.02 Implement Risk Based Decisions Process

Or

If "Full Controls":

AAA-08.03 Complete Nessus Scan/Nmap (Discovery Scan)

And

AAA-08.04 Complete Code Review Scan

And

AAA-08.05 Complete Penetration Test/Application Assessment

And

AAA-08.06 Complete Security Configuration Compliance Scan

Description

The System Owner determines if all of the security controls are needed.

Responsible Role

System Owner

Accountable Role

Office of Cyber Security Representative

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-08.02 Implement Risk Based Decisions Process

Previous Activities

AAA-08.01 All Security Controls Required?

Next Activities

AAA-08.03 Complete Nessus Scan/Nmap (Discovery Scan)

And

AAA-08.04 Complete Code Review Scan

And

AAA-08.05 Complete Penetration Test/Application Assessment

And

AAA-08.06 Complete Security Configuration Compliance Scan

Description

If System Owner elects not to implement any of the security controls based on the system's specific environments then the System Owner follows the Risk Based Decisions as specified in the Bulletin FSS No. 96, Types of Risk Based Decisions, and other guidance in the Office of Information Security (OIS) Risk Based Decisions Portal. For Local RBD the System Owner develops a RBD Memorandum justifying the reasons a security control was not implemented, and uploads the signed Memorandum to RiskVision.

For OIS/National RBD, the System Owner documents and signs justification as to why a common control or hybrid control cannot be implemented and includes recommended actions including any compensating controls, and completes the OIS/National RBD Memorandum template justifying reasons common or hybrid control are not implemented. The System Owner coordinates with ISO to request the Deputy Assistant Secretary, Information Security review and sign the memorandum. The System Owner, or delegate/System Steward, uploads the signed memorandum to RiskVision.

Input

Justification for not implementing Local or OIS/National Security Controls

Output

Local Risk Based Decision Memorandum

OIS Risk Based Decision Memorandum

Associated Artifacts

Local Risk Based Decision Memorandum

OIS Risk Based Decision Memorandum

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Office of Information Security Risk Based Decisions Portal

Standards

Bulletin FSS No. 96, Types of Risk Based Decisions

Office of Information Security Risk Based Decision Standard Operating Procedures

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

VA Handbook 6500, Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program

More Info

None Listed

Process Activity Name: AAA-08.03 Complete Nessus Scan/Nmap (Discovery Scan)

Concurrent Activities

AAA-08.04 Complete Code Review Scan

And

AAA-08.05 Complete Penetration Test/Application Assessment

And

AAA-08.06 Complete Security Configuration Compliance Scan

Previous Activities

AAA-08.01 All Security Controls Required?

Or

AAA-08.02 Implement Risk Based Decisions Process

Next Activities

AAA-08.07 SCA Required?

Description

The System Owner contacts the Certification Program Office (CPO) who requests a Nessus scan of the system from the Network and Security Operations Center (NSOC). A vulnerability and a discovery scan against all instantiations of the operating system and desktop configurations must be conducted to identify security flaws. All vulnerability scans that identify Critical and/or High deficiencies should be remediated or have a documented mitigation plan. System Owner or designee uploads scan results provided by NSOC, or by Enterprise Operations (EO) if performed locally, into RiskVision.

For each deficiency identified from the scan, System Owner or designee, creates a response for mitigating the deficiencies, a schedule for completion, status of each deficiency mitigated, and/or provide evidence that the deficiencies have been mitigated, and upload the deficiency states to RiskVision in a MS Word/Excel document.

Input

Request for a Scan

Output

Deficiencies Mitigation Descriptions

Scan Results

Supplemental Vulnerability Scan Request

Updated Deficiencies Spreadsheet in RiskVision

Associated Artifacts

Supplemental Vulnerability Scan Request Template

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision National Release GRC Instance

Agiliance RiskVision Enterprise Operations GRC Instance

Office of Cyber Security (OCS) Portal

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

CPO can be contacted via Certification PMO mail group.

Process Activity Name: AAA-08.04 Complete Code Review Scan

Concurrent Activities

AAA-08.03 Complete Nessus Scan/Nmap (Discovery Scan)

And

AAA-08.05 Complete Penetration Test/Application Assessment

And

AAA-08.06 Complete Security Configuration Compliance Scan

Previous Activities

AAA-08.01 All Security Controls Required?

Or

AAA-08.02 Implement Risk Based Decisions Process

Next Activities

AAA-08.07 SCA Required?

Description

The System Owner ensures a complete Code Review test is conducted on VA developed applications to identify security vulnerabilities, coding, and design flaws. System Owner, or delegate, contacts the National Service Desk (NSD) helpdesk to request a Fortify License. The System Owner, or delegate, conducts the final Fortify scan during the Assessment and Authorization process and provides the test result files (such as the Fortify scan files), along with the complete and buildable application source code for verification to the Office of Cyber Security (OCS) Software Assurance Team according to the Secure Code Review Standard Operating Procedures. All Critical and High deficiencies are mitigated with documented mitigation evidence provided, along with other requirements as defined in the Secure Code Review Standard Operating Procedures. Secure Code Review Validation reports and Plan of Action and Milestones (POAM) are uploaded to RiskVision.

Input

Secure Code Review

Output

Code Review Validation Submission Package

OIS V & V Secure Code Review Validation Request Form

Plan of Action and Milestones

Associated Artifacts

OIS V and V Secure Code Review Validation Request Form Template

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

OIS Software Assurance Portal

HP Fortify Static Code Analyzer (SCA)

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

Secure Code Review Standard Operating Procedure

More Info

Use the OIS Software Assurance Portal website and select Technical Notes to find how to information about:

1) Requesting Fortify software and 2) Requesting Secure Code Review Validations.

For more information about Secure Code Review policy and procedures, see the Secure Code Review Standard Operating Procedures.

Process Activity Name: AAA-08.05 Complete Penetration Test/Application Assessment

Concurrent Activities

AAA-08.03 Complete Nessus Scan/Nmap (Discovery Scan)

And

AAA-08.04 Complete Code Review Scan

And

AAA-08.06 Complete Security Configuration Compliance Scan

Previous Activities

AAA-08.01 All Security Controls Required?

Or

AAA-08.02 Implement Risk Based Decisions Process

Next Activities

AAA-08.07 SCA Required?

Description

The System Owner, or delegate, contacts Certification Program Office (CPO) to request Penetration Test/Application Assessment from Network and Security Operations Center (NSOC). A full test must be performed to include automated and manual assessment tools and techniques on Internet Facing and/or High Impact Applications. NSOC conducts the test and provides results to System Owner, designee, or system Points of Contact. System Owners should allow 30 days for NSOC to schedule/conduct the Penetration Test/Application Assessment. All Critical and High deficiencies are to be mitigated with documented mitigation evidence provided, and Moderate and Low deficiencies should be mitigated or have a documented mitigation plan. The System Owner or delegate coordinates the mitigation of deficiencies, documents mitigation plans, and uploads test results, mitigation evidence and plans to RiskVision.

Input

Penetration Test/Application Assessment Request

Output

Penetration Test Questionnaire

Test Results

Mitigation Plans

Mitigation Evidences

Associated Artifacts

Penetration Test Questionnaire Template

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

The Certification Program Office (CPO) can be contacted via CertificationPMO@va.gov.

Process Activity Name: AAA-08.06 Complete Security Configuration Compliance Scan

Concurrent Activities

AAA-08.03 Complete Nessus Scan/Nmap (Discovery Scan)

And

AAA-08.04 Complete Code Review Scan

And

AAA-08.05 Complete Penetration Test/Application Assessment

Previous Activities

AAA-08.01 All Security Controls Required?

Or

AAA-08.02 Implement Risk Based Decisions Process

Next Activities

AAA-08.07 SCA Required?

Description

The System Owner, or delegate, contacts Certification Program Office (CPO) to request Security Configuration Compliance Scan from Network and Security Operations Center (NSOC). Compliance scans must be performed against all Windows hosts (NSOC only has Windows Compliance scan capabilities) and must check against VA approved hardening guidance for the following:

- Operating Systems (DISA Security Technical Implementation Guides (STIG), NIST United States Government Configuration Baseline (USGCB), Microsoft) - Databases (DISA STIG, NIST USGCB, Microsoft) - Network / Security Devices (NSA Systems and Network Attack Center (SNAC) Configuration Guides) A compliance scan using an SCAP validated scanning tool must be conducted with a passing result and all compliance scans with failing results should have a documented mitigation plan. The System Owner or delegate is responsible for

coordinating the mitigation of deficiencies, documenting the mitigation plans, and uploading them to RiskVision.

Input

Security Configuration Compliance Scan Request

Output

Completed Security Configuration Compliance Scan

Test Results

Mitigation Plans

Mitigation Evidence

Associated Artifacts

None Listed

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision National Release GRC Instance

Agiliance RiskVision Enterprise Operations GRC Instance

Office of Cyber Security (OCS) Portal

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

The Certification Program Office (CPO) can be contacted via CertificationPMO@va.gov.

Process Activity Name: AAA-08.07 SCA Required?

Previous Activities

AAA-08.03 Complete Nessus Scan/Nmap (Discovery Scan)

Or

AAA-08.04 Complete Code Review Scan

Or

AAA-08.05 Complete Penetration Test/Application Assessment

Or

AAA-08.06 Complete Security Configuration Compliance Scan

Next Activities

If "Yes":

AAA-08.08 Complete Security Control Assessment

Or

If "No":

AAA-10 Review Security Controls

Description

The Office of Cyber Security Representative determines if a Security Control Assessment (SCA) is required.

Responsible Role

Office of Cyber Security Representative

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-08.08 Complete Security Control Assessment

Previous Activities

AAA-08.07 SCA Required?

Next Activities

AAA-10 Review Security Controls

Description

Office of Cyber Security (OCS) Representative determines if a Security Control Assessment (SCA) is required. If an SCA is required, OIT Enterprise Risk Management (ERM) is notified by OCS to schedule and conduct the SCA, and will provide the results to the System Owner, delegate, or System Point of Contacts. System Owner or delegate is responsible for coordinating the mitigation of deficiencies, documenting the mitigation plans, and uploading them along with the test results to RiskVision. All Critical and High Plan of Action and Milestones (POA&M)

should be mitigated with documented mitigation evidence provided, and Moderate and Low POA&Ms should be mitigated or have a documented mitigation plan.

Input

Security Control Assessment Request

Output

Completed Security Control Assessment

Mitigation Evidence

Mitigation Plans

Test Results

Associated Artifacts

None Listed

Responsible Role

Office of Cyber Security Representative

Accountable Role

Information Security Officer

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision National Release GRC Instance

Agiliance RiskVision Enterprise Operations GRC Instance

Office of Cyber Security (OCS) Portal

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

None Listed

Process Activity Name: AAA-09 Complete Application Registration

Previous Activities

AAA-06 Obtain Access to the GRC Tool

Or

AAA-12 Inform System Owner

Next Activities

AAA-10 Review Security Controls

Description

The System Owner ensures VA developed applications are registered with the VA Software Assurance Program Office, including those written in MUMPS or Delphi, per “Software Assurance Program Memorandum" (VAIQ #7477488), signed by Stephen Warren, on April 10, 2015. Registration is necessary to maintain an inventory of the total population of VA custom applications, by type and business line according to the VA Common Application Enumeration (CAE) to ensure application-level security considerations are taken into account when determining readiness and performance.

Input

VA Developed Application Registration

Output

VA Developed Application Registration Request Form

Associated Artifacts

None Listed

Responsible Role

System Owner

Accountable Role

Information Security Officer

Consulted Role

Office of Cyber Security Representative

Informed Role

Director, Certification Program Office; Director, Office of Cyber Security

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

OIS Software Assurance Portal

HP Fortify Static Code Analyzer (SCA)

Standards

Secure Code Review Standard Operating Procedure

Office of Information Security Risk Based Decision Standard Operating Procedures

VA Common Application Enumeration

Software Assurance Program Memorandum (VAIQ 7477488)

More Info

Use the OIS Software Assurance Portal website and select Technical Notes to find further information about Registering VA Developed Applications.

For more information about Secure Code Review policy and procedures, see the Secure Code Review Standard Operating Procedures.

For a sample of a VA Developed Application Registration Request form please see:

https://wiki.mobilehealth.va.gov/display/OISSWA/How+to+open+an+NSD+ticket+to+register+a+VA+application

Process Activity Name: AAA-10 Review Security Controls

Previous Activities

AAA-07 Assemble Required Artifacts

Or

AAA-08 Complete Technical/Testing Requirements

Or

AAA-09 Complete Application Registration

Next Activities

AAA-11 Completed?

Description

The Information Security Officer reviews the completed accreditation requirements including security artifacts, technical/testing, and security control assessment in the Accreditation Package in the Governance, Risk and Compliance (GRC) Tool for completion and correctness. If there are any pending issues, the System Owner is notified to resolve them; otherwise, the Certification Agents are notified to review the submitted package in the GRC tool.

Input

Accreditation Package

Output

Reviewed Accreditation Package

Associated Artifacts

None Listed

Responsible Role

Information Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

None Listed

Process Activity Name: AAA-11 Completed?

Previous Activities

AAA-10 Review Security Controls

Next Activities

If "No":

AAA-12 Inform System Owner

Or

If "Yes":

AAA-13 Obtain Approval

Description

It is determined if the Accreditation Package is complete.

Responsible Role

Information Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-12 Inform System Owner

Previous Activities

AAA-11 Completed?

Or

AAA-14 Approved?

Next Activities

AAA-07 Assemble Required Artifacts

And

AAA-08 Complete Technical/Testing Requirements

And

AAA-09 Complete Application Registration

Description

The Information Security Officer informs and supports the System Owner to resolve any pending issues with the submitted accreditation artifacts and technical testing results.

Input

Accreditation Package

Output

Action Items to resolve pending discrepancies

Associated Artifacts

None Listed

Responsible Role

Information Security Officer

Accountable Role

Certification Agent

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

None Listed

Process Activity Name: AAA-13 Obtain Approval

Previous Activities

AAA-11 Completed?

Next Activities

AAA-13.01 Review Security Controls

Description

This group of activities focuses on the reviews and obtaining approval of the ATO.

Process Activity Name: AAA-13.01 Review Security Controls

Previous Activities

AAA-13 Obtain Approval

Next Activities

AAA-13.02 Approved?

Description

The Certification Agent reviews and verifies the completed Security Controls and Accreditation Requirements Artifacts submitted to RiskVision (Accreditation Package). Should there be any issues, the Information Security Officer is notified to inform the System Owner. Otherwise, the Director of Certification Program Office is notified to review submitted material.

Input

Accreditation Package

Output

Reviewed Accreditation Package

Associated Artifacts

None Listed

Responsible Role

Certification Agent

Accountable Role

Director, Certification Program Office

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

None Listed

Process Activity Name: AAA-13.02 Approved?

Previous Activities

AAA-13.01 Review Security Controls

Next Activities

If "Yes":

AAA-13.03 Review Security Controls

Or

If "No":

AAA-14 Approved?

Description

The Certification Agent reviews the completed Security Controls and Accreditation Requirements Artifacts submitted to RiskVision (Accreditation Package). If approved, the Accreditation Package is submitted to the Director of Certification Program Office to review. If not approved, the package is sent to the Information Security Officer.

Responsible Role

Certification Agent

Accountable Role

Director, Certification Program Office

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-13.03 Review Security Controls

Previous Activities

AAA-13.02 Approved?

Next Activities

AAA-13.04 Approved?

Description

The Director of Certification Program Office reviews and verifies the completed Security Controls and Accreditation Requirements Artifacts submitted to RiskVision (Accreditation Package). If they are any issues, the Information Security Officer is notified to inform the System Owner; otherwise, the Director of Office of Cyber Security is notified to review submitted material.

Input

Accreditation Package

Output

Reviewed Accreditation Package

Associated Artifacts

None Listed

Responsible Role

Director, Certification Program Office

Accountable Role

Director, Office of Cyber Security

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

Office of Information Security, Accreditation Requirements Guide Standard Operating Procedures

More Info

None Listed

Process Activity Name: AAA-13.04 Approved?

Previous Activities

AAA-13.03 Review Security Controls

Next Activities

If "Yes":

AAA-13.05 Review Security Controls

Or

If "No":

AAA-14 Approved?

Description

The Director of Certification Program Office reviews the completed Security Controls and Accreditation Requirements Artifacts submitted to RiskVision (Accreditation Package). If approved, the Accreditation Package is submitted to the Director of office of Cyber Security to review. If not approved, the package is sent to the Information Security Officer.

Responsible Role

Director, Certification Program Office

Accountable Role

Director, Office of Cyber Security

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-13.05 Review Security Controls

Previous Activities

AAA-13.04 Approved?

Next Activities

AAA-13.06 Approved?

Description

The Director of Office of Cyber Security reviews and verifies the completed Security Controls and Accreditation Requirements Artifacts submitted to RiskVision (Accreditation Package). If they are any issues the Information Security Officer is notified to Inform the System Owner.

Otherwise, the Deputy Assistant Secretary for Office of Information Security is notified to review submitted material.

Input

Accreditation Package

Output

Reviewed Accreditation Package

Associated Artifacts

None Listed

Responsible Role

Director, Office of Cyber Security

Accountable Role

Deputy Assistant Secretary, Office of Information Security

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

None Listed

More Info

None Listed

Process Activity Name: AAA-13.06 Approved?

Previous Activities

AAA-13.05 Review Security Controls

Next Activities

If "Yes":

AAA-13.07 Review Security Controls

Or

If "No":

AAA-14 Approved?

Description

The Director of Office of Cyber Security reviews the completed Security Controls and Accreditation Requirements Artifacts submitted to RiskVision (Accreditation Package). If approved, the Accreditation Package is submitted to the Deputy Assistant Secretary, Office of Information Security to review. If not approved, the package is sent to the Information Security Officer.

Responsible Role

Director, Office of Cyber Security

Accountable Role

Deputy Assistant Secretary, Office of Information Security

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-13.07 Review Security Controls

Previous Activities

AAA-13.06 Approved?

Next Activities

AAA-13.08 Approved?

Description

The Deputy Assistant Secretary for Office of Information Security reviews and verifies the completed Security Controls and Accreditation Requirements Artifacts submitted to RiskVision (Accreditation Package). If they are any issues, the Information Security Officer is notified to inform the System Owner. Otherwise, the Assistant Secretary for Information and Technology is notified to review submitted material.

Input

Accreditation Package

Output

Reviewed Accreditation Package

Associated Artifacts

None Listed

Responsible Role

Deputy Assistant Secretary, Office of Information Security

Accountable Role

Assistant Secretary for Information and Technology

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

None Listed

More Info

None Listed

Process Activity Name: AAA-13.08 Approved?

Previous Activities

AAA-13.07 Review Security Controls

Next Activities

If "Yes":

AAA-13.09 Review Security Controls

Or

If "No":

AAA-14 Approved?

Description

The Deputy Assistant Secretary, Office of Information Security reviews the completed Security Controls and Accreditation Requirements Artifacts submitted to RiskVision (Accreditation Package). If approved, the Accreditation Package is submitted to the Deputy Assistant Secretary, Office of Information Security to review. If not approved, the package is sent to the Information Security Officer.

Responsible Role

Deputy Assistant Secretary, Office of Information Security

Accountable Role

Assistant Secretary for Information and Technology

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-13.09 Review Security Controls

Previous Activities

AAA-13.08 Approved?

Next Activities

AAA-13.10 Approved?

Description

The Assistant Secretary for Information and Technology reviews the completed Security Controls and Accreditation Requirements artifacts submitted to RiskVision (Accreditation Package) and determines if an Authority to Operate memorandum could be issued for the system.

Input

Completed Accreditation Package

Output

Reviewed Accreditation Package

Associated Artifacts

None Listed

Responsible Role

Assistant Secretary for Information and Technology

Accountable Role

Assistant Secretary for Information and Technology

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

None Listed

More Info

None Listed

Process Activity Name: AAA-13.10 Approved?

Previous Activities

AAA-13.09 Review Security Controls

Next Activities

If "Yes":

AAA-13.11 Deny ATO

Or

If "No":

AAA-13.12 Approve ATO/TATO

Description

The Assistant Secretary for Information and Technology reviews the Accreditation Package. If approved, the ATO/TATO is approved. Otherwise, the ATO/TATO is denied.

Responsible Role

Assistant Secretary for Information and Technology

Accountable Role

Assistant Secretary for Information and Technology

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-13.11 Deny ATO

Previous Activities

AAA-13.10 Approved?

Next Activities

AAA-14 Approved?

Description

The Assistant Secretary for Information and Technology denies the Authority to Operate (ATO) for the system and the result is conveyed to the Certification Agent.

Input

Accreditation Package

Output

Denial of Authority to Operate

Associated Artifacts

None Listed

Responsible Role

Assistant Secretary for Information and Technology

Accountable Role

Assistant Secretary for Information and Technology

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

None Listed

More Info

None Listed

Process Activity Name: AAA-13.12 Approve ATO/TATO

Previous Activities

AAA-13.10 Approved?

Next Activities

AAA-14 Approved?

Description

The Assistant Secretary for Information and Technology approves a full Authority to Operate (ATO) or Temporary Authority to Operate (TATO) for the system and the result is conveyed to the Certification Agent.

Input

Accreditation Package

Output

Approval of Authority to Operate

Associated Artifacts

None Listed

Responsible Role

Assistant Secretary for Information and Technology

Accountable Role

Assistant Secretary for Information and Technology

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

None Listed

More Info

None Listed

Process Activity Name: AAA-14 Approved?

Previous Activities

AAA-13.11 Deny ATO

Or

AAA-13.12 Approve ATO/TATO

Next Activities

If "Yes":

AAA-15 Inform System Owner of ATO Status

Or

If "No":

AAA-12 Inform System Owner

Description

The Certification Agent verifies if the Accreditation Package is approved.

Responsible Role

Certification Agent

Accountable Role

Director, Certification Program Office

Consulted Role

None Listed

Informed Role

None Listed

Process Activity Name: AAA-15 Inform System Owner of ATO Status

Previous Activities

AAA-14 Approved?

Next Activities

Process Ends

Description

The Certification Agent notifies the System Owner of the Authority to Operate (ATO) adjudication by the Assistant Secretary for Information and Technology.

Input

Reviewed Accreditation Package

Output

Result of ATO Adjudication

Associated Artifacts

None Listed

Responsible Role

Certification Agent

Accountable Role

Director, Certification Program Office

Consulted Role

None Listed

Informed Role

None Listed

Tools and Websites

Agiliance RiskVision Enterprise Operations GRC Instance

Agiliance RiskVision National Release GRC Instance

Office of Cyber Security (OCS) Portal

Standards

None Listed

More Info

None Listed

END OF PROCESS